

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

25. 3. 2004

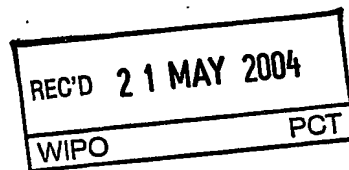
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日  
Date of Application: 2003年 3月26日

出 願 番 号  
Application Number: 特願2003-085043  
[ST. 10/C]: [JP2003-085043]

出 願 人  
Applicant(s): 松下電器産業株式会社

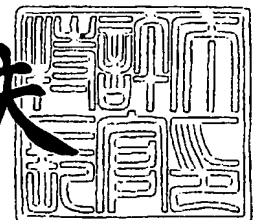


PRIORITY DOCUMENT  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH  
RULE 17.1(a) OR (b)

2004年 4月28日

特許庁長官  
Commissioner,  
Japan Patent Office

今 井 康 夫



【書類名】 特許願  
【整理番号】 2113140223  
【提出日】 平成15年 3月26日  
【あて先】 特許庁長官殿  
【国際特許分類】 H04N 7/167  
H04K 1/00  
G06F 12/14 320

## 【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 鈴木 秀和

## 【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

## 【代理人】

【識別番号】 100097445

## 【弁理士】

【氏名又は名称】 岩橋 文雄

## 【選任した代理人】

【識別番号】 100103355

## 【弁理士】

【氏名又は名称】 坂口 智康

## 【選任した代理人】

【識別番号】 100109667

## 【弁理士】

【氏名又は名称】 内藤 浩樹

## 【手数料の表示】

【予納台帳番号】 011305

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9809938

**【書類名】 明細書****【発明の名称】** リボケーション情報の送信方法、受信方法及びその装置**【特許請求の範囲】**

**【請求項 1】** コンテンツを送出するコンテンツ送出機器と、コンテンツ受信するコンテンツ受信機器と、前記コンテンツ機器と前記コンテンツ受信機器とを接続する接続手段から構成されるシステムにおいて、前記コンテンツ送出機器とコンテンツ受信機器が相互認証を行なうステップと、相互認証が失敗の場合、前記コンテンツ送出機器または前記コンテンツ受信機器から、相互認証に失敗した鍵情報を含みリボケーション情報をアップロードするステップと、複数のコンテンツ送出機器またはコンテンツ受信機器からアップロードされた個々のリボケーション情報を統合して統合リボケーション情報を作成するステップと、前記統合リボケーション情報をパケット化し、ストリームに多重するステップと、前記統合リボケーションが多重されたストリームを送出するステップを備えることを特徴とするリボケーション情報の送信方法。

**【請求項 2】** 1 個または複数のコンテンツ送出機器またはコンテンツ受信機器のリボケーション情報を統合して統合リボケーション情報を作成するステップと、前記統合リボケーション情報を前記統合リボケーション情報をパケット化し、ストリームに多重するステップと、前記統合リボケーションが多重されたストリームを送出するステップを備えることを特徴とするリボケーション情報の送信方法。

**【請求項 3】** 統合リボケーション情報を M P E G トランスポートストリームのセクションのデータ構造を用いて伝送することを特徴とする請求項 1 または請求項 2 に記載のリボケーション情報の送信方法。

**【請求項 4】** 統合リボケーション情報を M P E G トランスポートストリームの P E S パケットのデータ構造を用いて伝送することを特徴とする請求項 1 または請求項 2 に記載のリボケーション情報の送信方法。

**【請求項 5】** 統合リボケーション情報を M P E G トランスポートストリームのトランスポートパケットのペイロードを用いて伝送することを特徴とする請求項 1 または請求項 2 に記載のリボケーション情報の送信方法。

【請求項 6】 統合リボケーション情報を IP パケットを用いて伝送することを特徴とする請求項 1 または請求項 2 に記載のリボケーション情報の送信方法。

【請求項 7】 コンテンツ送出機器またはコンテンツ受信機器が統合リボケーションリストを受信し、前記コンテンツ送出機器または前記コンテンツ受信機器が前記統合リボケーションリストを記憶することを特徴とするリボケーション情報の受信方法。

【請求項 8】 コンテンツを送出する複数のコンテンツ送出機器と、前記複数のコンテンツ送出機器にそれぞれ接続され、コンテンツを受信する複数のコンテンツ受信機器と、前記コンテンツ送出機器と前記コンテンツ受信機器とを接続する接続手段と、前記複数のコンテンツ送出機器または前記複数の受信機器からリボケーション情報を吸い上げるネットワークと前記ネットワークに接続され、リボケーション情報を統合する統合手段と、前記統合手段において統合された統合リボケーション情報をパケット化してストリームに多重する多重化手段と、前記多重化手段において多重されたストリームを送信する送信手段とを備えることを特徴とするリボケーション情報の送信装置。

【請求項 9】 1 個または複数のコンテンツ送出機器またはコンテンツ受信機器のリボケーション情報を統合する統合手段と、前記統合手段において統合された統合リボケーション情報をパケット化してストリームに多重する多重化手段と、前記多重化手段において多重されたストリームを送信する送信手段とを備えることを特徴とするリボケーション情報の送信装置。

【請求項 10】 統合リボケーション情報を MPEG トランスポートストリームのセクションのデータ構造を用いて伝送することを特徴とする請求項 8 または請求項 9 に記載のリボケーション情報の送信装置。

【請求項 11】 統合リボケーション情報を MPEG トランスポートストリームの PES パケットのデータ構造を用いて伝送することを特徴とする請求項 8 または請求項 9 に記載のリボケーション情報の送信装置

【請求項 12】 統合リボケーション情報を MPEG トランスポートストリームのトランスポートパケットのペイロードを用いて伝送することを特徴とする請

求項 8 または請求項 9 に記載のリボケーション情報の送信装置。

【請求項 13】 統合リボケーション情報を IP パケット用いて伝送することを特徴とする請求項 8 または請求項 9 に記載のリボケーション情報の送信装置。

【請求項 14】 コンテンツ送出機器またはコンテンツ受信機器が統合リボケーションリストを受信し、前記コンテンツ送出機器または前記コンテンツ受信機器が前記統合リボケーションリストを記憶することを特徴とするリボケーション情報の受信装置。

#### 【発明の詳細な説明】

##### 【0001】

#### 【発明の属する技術分野】

この発明は、デジタル映像やデジタル音声を不当な電子機器で表示したり、再生したりすることを防止するためのリボケーション情報の配信方法及び装置に関するものである。

##### 【0002】

#### 【従来の技術】

近年、デジタル技術の発展に伴って、デジタル放送やインターネットによるデジタルコンテンツの配信や、DVD やハードディスクやメモリカードによるデジタルコンテンツの配布や蓄積が盛んに行なわれている。これらのメディアではデジタルデータを用いるので、その品質を劣化させることなくコピーを行なうことが可能であるが、著作権保護の観点からその不正なコピーを防ぐためのセキュリティの実現が重要である。セキュリティの実現のためには、著作権保護上、不正な機器が発覚した場合、不正機器のいわゆるブラックリストであるリボケーション情報を発行し、不正な機器に接続されうる機器がそのリボケーション情報を持ち、デジタルコンテンツへの不正なアクセスを防ぐ必要がある。

##### 【0003】

リボケーション情報の更新に関する従来例のシステムの構成を図 25 に示す（特許文献 1 参照）。

##### 【0004】

1 はコンテンツ販売システムで、放送やインターネットの通信網を介して音楽

コンテンツを電子配信する自動販売機である。2はElectric MUSIC Distributer (EMD)で音楽サーバーや音楽放送局である。3はリボケーション情報発行機関である。4はセキュアコンテンツサーバーである。5はリボケーション情報格納部で、リボケーション情報発行機関が発行したりリボケーション情報を受け取る。6は音楽データ格納部で、音楽データを格納する。7はライセンス格納部で、暗号化コンテンツを復号するためのキーを格納する。8はEMD I/F部で暗号化コンテンツを受け取るためのインタフェースである。9はPD I/F部でPD12と接続するためのインタフェースである。10はメディアI/F部でPM13を装着するためのPCMCIAのカードスロットである。11は記憶メディアで、Portable Media (PM)である。12は記憶再生装置PDである。13はユーザI/F部でユーザが操作を行うインタフェースである。

#### 【0005】

#### 【特許文献1】

特開2001-166996号公報

#### 【0006】

#### 【発明が解決しようとする課題】

しかし、この従来例ではリボケーション情報の更新方法については述べられているが、リボケーション情報を配布する具体的方法がないため、デジタル放送やインターネットでのコンテンツ配信が高まりを見せる状況で、リボケーション情報の配信するための必要がある。

#### 【0007】

#### 【課題を解決するための手段】

本発明は上記の問題点を解決するためになされたもので、本発明（請求項1）にかかるリボケーション情報の送信方法は、コンテンツを送出するコンテンツ送出機器と、コンテンツ受信するコンテンツ受信機器と、前記コンテンツ機器と前記コンテンツ受信機器とを接続する接続手段から構成されるシステムにおいて、前記コンテンツ送出機器とコンテンツ受信機器が相互認証を行なうステップと、相互認証が失敗の場合、前記コンテンツ送出機器または前記コンテンツ受信機器

から、相互認証に失敗した鍵情報を含みリボケーション情報をアップロードするステップと、複数のコンテンツ送出機器またはコンテンツ受信機器からアップロードされた個々のリボケーション情報を統合して統合リボケーション情報を作成するステップと、前記統合リボケーション情報をパケット化し、ストリームに多重化するステップと、前記統合リボケーションが多重されたストリームを送出するステップを備えることを特徴とする。

#### 【0008】

また本発明（請求項7）にかかるリボケーション情報の受信方法は、コンテンツ送出機器またはコンテンツ受信機器が統合リボケーションリストを受信し、前記コンテンツ送出機器または前記コンテンツ受信機器が前記統合リボケーションリストを記憶することを特徴とする。

#### 【0009】

また、本発明（請求項8）にかかるリボケーション情報の送信装置は、コンテンツを送出する複数のコンテンツ送出機器と、前記複数のコンテンツ送出機器にそれぞれ接続され、コンテンツを受信する複数のコンテンツ受信機器と、前記コンテンツ送出機器と前記コンテンツ受信機器とを接続する接続手段と、前記複数のコンテンツ送出機器または前記複数の受信機器からリボケーション情報を吸い上げるネットワークと前記ネットワークに接続され、リボケーション情報を統合する統合手段と、前記統合手段において統合された統合リボケーション情報をパケット化してストリームに多重する多重化手段と、前記多重化手段において多重されたストリームを送信する送信手段とを備えることを特徴とする。

#### 【0010】

また、本発明（請求項14）にかかるリボケーション情報の受信装置は、コンテンツ送出機器またはコンテンツ受信機器が統合リボケーションリストを受信し、前記コンテンツ送出機器または前記コンテンツ受信機器が前記統合リボケーションリストを記憶することを特徴とする。

#### 【0011】

##### 【発明の実施の形態】

##### （実施の形態1）



以下、図面を参照しながら本発明のリボケーション情報の送信方法、受信方法の実施の形態1について説明する。図1は本発明の実施の形態1におけるリボケーション情報の送信方法、受信方法を実現するシステムの構成を示す図である。

101～109は各家庭にある民生機器である。101は第1のディスプレイで、CRTや液晶ディスプレイ、プラズマディスプレイ等で映像を表示するもので、スピーカも備え音声を出力する場合もある。

#### 【0012】

図2に第1のディスプレイ101の内部構成を示す。1001は表示部で映像を表示するものである。1002は機器インタフェースで後述するSTBと接続するものである。1003はディスプレイのコントロール部で、ディスプレイ全体の制御を行うものである。1004はメモリ部で、後述するディスプレイのメーカIDや機器IDや鍵情報を格納するものである。

#### 【0013】

102は第1のSTB（セットトップボックス）で、配信または放送されるデジタルの映像や音声その他のデータを受信し、復号、再生を行うものである。ここではデジタル放送を受信するSTBとする。

#### 【0014】

図3にSTBの内部構成を示す。1101はアンテナでデジタル放送の電波を受信するものである。1102はチューナー部で、放送波の復調を行うものである。1103はフロントエンド部で、復調された信号に対して、誤り訂正等を行いTS（トランスポートストリーム）を再生するものである。1104はTSデコーダ部で、複数の番組が多重されたTSからユーザが選択した番組のパケット（映像、音声、データ等）を抽出するものである。1105はAVデコーダ部で、TSデコーダ部1104で抽出した映像パケット及び音声パケットの伸張を行い、デジタルの映像信号及び音声信号を出力するものである。1106はコントロール部で、STBの全体の制御を行うものである。1107はメモリ部で後述するリボケーションリストやSTBの鍵情報など格納するものである。1108はディスプレイインタフェースで映像、音声をディスプレイに向けて出力したり、鍵情報を交換したりするためのものである。1109はモデム部で、後述する

ネットワーク 113 と通信するためのものである。

【0015】

103 は第1のディスプレイと第1のSTBを接続するデジタルインタフェースであり、ここでは例としてHDMI (High-Definition Multimedia Interface) とする。104 は第2のディスプレイで、第1のディスプレイ101と同様なものである。105 は第2のSTBで、第1のSTB102と同様なものである。106 は第2のディスプレイと第2のSTBを接続する第2のデジタルインタフェースで、第1のデジタルインタフェース103と同一である。

【0016】

107 は第Nのディスプレイ (Nは自然数) で、第1のディスプレイ101と同様なものである。108 は第NのSTBで、第1のSTB102と同様なものである。109 は第Nのデジタルインタフェースで、第1のデジタルインタフェース103と同様なものである。

【0017】

110 は第1のSTB102と後述するネットワークとを接続する第1の上り回線で、STBに蓄積したリボケーションリストをネットワークに送信するための媒体である。リボケーションリストについては後で説明する。上り回線には銅線や光ケーブル等がある。

【0018】

111 は第2の上り回線で、第1の上り回線110と同様なものである。112 は第Nの上り回線で、第1の上り回線110と同様なものである。101~112 は各家庭に存在するものまたは、各家庭個別に対応するものであり、Nの値は限定されるものではない。

【0019】

113 はネットワークで、各家庭のSTBからリボケーションリストのリボケーションリスト統合部に吸い上げるための媒体であり、例えば電話網やインターネットなどがある。114 はリボケーションリスト統合部で各STBから吸い上げられたリボケーションリストを統合して、リボケーションリストの一覧である

統合リボケーションリストの作成及び管理を行うものである。115は送出センターで、統合されたりボケーションリストをパケット化して放送用のトランスポートストリームに多重するものである。116は送信部で、各STBに送信するもので、例えば送信アンテナである。

#### 【0020】

以上のように構成された実施の形態1についてその動作を説明する。HDMIではHDCP (High-Bandwidth Digital Content Protection) という暗号化システムが用いられる。HDCPは、STBやDVDといった映像や音声を送出する送出機器と、ディスプレイなど映像を表示する受信機器との間に流れるデジタルコンテンツの暗号化方法を規定する。詳細はHDCPの規格書である、High-Bandwidth Digital Content Protection System、に詳述されており説明を省略する。

#### 【0021】

第1～第Nのディスプレイは、それぞれのメモリ部1104に、メーカーID、機器ID及び56ビット×40行のディスプレイ用のデバイスキーの行列を有している。この様子を図4に示す。また、このデバイスキーの行列に対応して、個々のデバイスキーの行を指定するためのキーセレクションベクトル（以下KSVと略す）が割り当てられ、メモリ部1107に格納されている。以降、ディスプレイ用のKSVをBk s vと記す。

#### 【0022】

また第1～第NのSTBもそれぞれのメモリ部1004にSTB用のデバイスキーとKSVを有している。以降、STB用のKSVをAk s vと記す。

#### 【0023】

デバイスキーもキーセレクションベクトルも、HDCPの管理組織であるLLCが管理し、各ディスプレイやSTBやDVDといった各機器に付与する。

#### 【0024】

次に各STBでのリボケーションリストの作成の方法について説明する。例として、第1のSTB102と第1のディスプレイ101について説明する。図5

にSTBとディスプレイの初期認証の処理を示す。この処理の詳細は先述した文献Higier-Bandwidth Digital Content Protection Systemに述べられており、説明を省略する。第1のSTBがメモリ部1107に有しているリボケーションリストの例を図6に示す。このリストには、著作権保護上、不正機器として排除すべきディスプレイのメーカーID、機器ID、Bksvが格納されており、図6の例では2個のディスプレイが排除されるべき機器として登録されている。メーカーIDはメーカを識別するものである。機器IDは機器を識別するもので例えば機器のシリアルナンバーである。

#### 【0025】

以下、初期認証について説明する。まず、第1のSTB102と第1のディスプレイ101が第1のデジタルインタフェース103で接続されるか、または第1のSTB102と第1のディスプレイ101に電源が投入される。

#### 【0026】

次に第1のSTB102は第1のディスプレイ101からメーカーID、機器ID、Bksvを第1のデジタルインタフェース103を介して読み出す。このとき、第1のデジタルインタフェースの制御線であるI2Cラインを用いればよい。

#### 【0027】

ここで、読み出したメーカーID、機器ID、Bksvが第1のSTBが持っているリボケーションリストに同一のものがあれば、初期認証は失敗として、以降そのディスプレイを使用できなくする。

#### 【0028】

次に、第1のSTB102から第1のディスプレイ101に対して、64ビットの乱数Anと、Aksvを第1のデジタルインタフェース103経由で書き込む。

#### 【0029】

ここでもI2Cラインを用いればよい。

#### 【0030】

次に、第1のSTB102は第1のディスプレイ101からBk s vを読み出し、第1のSTBで、下記(数1)の演算を行なう。

【0031】

【数1】

$$K_m = \Sigma A_{\text{keys over Bk s v}}$$

【0032】

(数1)の演算を説明する。A k e y sはSTBのメモリ部1107に格納されている56ビット×40行のSTBのデバイスキーの行列である。例えばB k s vを16進数表現で0×2B8とすれば、ゼロ始まりでのビット位置3, 4, 5, 7, 9のみ1であとは0である。

【0033】

そして、上の式はB k s vの1が存在するビット位置3, 4, 5, 7, 9を行のインデクスとして、5個の56ビットのキーを加算したものである。

【0034】

第1のディスプレイ101でも、同様に下記(数2)の演算を行なう。

【0035】

【数2】

$$K_m' = \Sigma B_{\text{keys over Aksv}}$$

【0036】

B k e y sはディスプレイのメモリ部1004に格納されている56ビット×40行のディスプレイのデバイスキーの行列である。

【0037】

次にSTBではK<sub>m</sub>をもとにして、下記(数3)の演算を行ない、K<sub>s</sub>、M<sub>0</sub>、R<sub>0</sub>を得る。

【0038】

【数3】

$$(K_s, M_0, R_0) = \text{hdcpBlkCipher}(K_m, \text{REPEATER} || A_n)$$

【0039】

(数3)でREPEATERは該当する機器がリピート機能、つまり再送信機

能を果たす場合に1で、それ以外の場合は0である。ここではディスプレイがリピート機能を有さないとし、0とする。また(数3)で||はビットの連結を示す。(数3)で用いられるhdc p B l k C i p h e rという演算子については、文献H i g h - B a n d w i d t h D i g i t a l C o n t e n t P r o t e c t i o n S y s t e mの4. 5節に詳述されているので説明を省略する。

#### 【0040】

一方、ディスプレイでも同様に下記(数4)の演算を行なう。

#### 【0041】

#### 【数4】

$(Ks', M0', R0') = \text{hdc p B l k C i p h e r}(Km', \text{REPEATER} || An)$

#### 【0042】

次に初期認証の判定処理を行なうが、この様子を図7に示す。STBはディスプレイからR0'を読み出し、R0=R0'であるかどうかを判定する。もしR0とR0'が一致すれば、初期認証は成功である。一方、R0とR0'が一致しなければ、初期認証は失敗とし、STBはメモリ部1107のリボケーションリストにディスプレイのBk s vを違反しているものとして登録する。このとき、メーカーIDと機器IDも併せて格納する。その場合のメモリ部1107の様子を図8に示す。図8において、m a k e r \_ 3、k i k i \_ 3、B k s v \_ 3が新たな不正機器として登録されたものである。

#### 【0043】

以上の初期認証処理の詳細は文献H i g h - B a n d w i d t h D i g i t a l C o n t e n t P r o t e c t i o n S y s t e mに詳述されているので説明を省略する。第2～第NのSTB、第2～第Nのディスプレイでも、第1のSTB、第1のディスプレイと同様な初期認証処理を行ない、違反しているBk s vがあれば、それらに接続されたSTBのメモリ部のリボケーションリストに登録する。

#### 【0044】

次に各STBに登録されているリボケーションリストを統合して、各STBに

送信する方法について説明する。図9にリボケーションリストのアップロード～送出までのフローを示す。

#### 【0045】

ステップ101において、

STBのコントロール部1106が、メモリ部1107に格納されたりボケーションリストからメーカーID、機器ID、Bksvを読み出し、モデム部1109に転送する。

#### 【0046】

ステップ102において、

STBのモデム部1109から上り回線110、ネットワーク113経由でBksvをリボケーションリスト統合部114にアップロードする。

#### 【0047】

ステップ103において、

リボケーションリスト統合部114において、所定期間に各STBからアップロードされたBksvのリストを作成し、これを統合リボケーションリストとする。

#### 【0048】

ステップ104において、

リボケーションリスト統合部114から送出センター115に統合リボケーションリストを伝送する。

#### 【0049】

ステップ105において、

送出センター115で統合リボケーションリストをパケット化して、トランスポートストリームに多重する。

#### 【0050】

ステップ106において、

送信部116より、統合リボケーションリストが多重されたトランスポートストリームを各STBに送信する。

#### 【0051】

ここでステップ105におけるリボケーションリストのパケット化及び多重化

について詳細に説明する。図10にトランスポートパケットの模式図を示し、図11にトランスポートパケットのデータ構造を示す。トランスポートパケットのデータ構造は、MPEGシステム規格書であるISO/IEC13818-1に述べられているので省略する。

#### 【0052】

統合リボケーションリストはトランスポートパケットのペイロード部分すなわち、図10のdata\_byteの部分に格納し、ある所定のPIDを割り当てる。このPIDを仮にRevocation\_pidとする。実施の形態1では統合リボケーションリストはMPEGシステム規格のセクション構造に格納する。図11に統合リボケーションリストをセクション構造に格納した場合のデータ構造の例を示す。統合リボケーションリストのテーブルを仮にRevocation\_list\_tableと称するが、もちろん、他の名前であっても構わない。このデータ構造において、maker\_id(16ビット)、kiki\_id(32ビット)、device\_KSV(40ビット)がSTBから吸い上げた、メーカーID、機器ID、違反した個々のBksvである。ただし、メーカーID、機器IDは何ビットであっても構わない。

#### 【0053】

次に、各STBにおける統合リボケーションリストの受信の方法について説明する。図13にSTBでの統合リボケーションリストの受信フローを示す。

#### 【0054】

ステップ201において、

STBがRevocation\_list\_tableを含むTS(トランスポートストリーム)を受信する。

#### 【0055】

ステップ202において、

STBのTSデコーダ部1104でTSからRevocation\_list\_tableを含むパケットを抽出するように、コントロール部1106は、TSデコーダ部1104にPIDフィルタにRevocation\_pidを設定する。PIDフィルタとは、指定したPIDを持ったパケットを抽出するもの



でTSデコーダには必須の機能ある。

#### 【0056】

ステップ203において、

TSデコーダ部でRevocation\_list\_tableを含むパケットを抽出し、コントロール部1106が統合リボケーションリストを取得する。

#### 【0057】

ステップ204において、

コントロール部1106は取得した統合リボケーションリストを、メモリ部1107に格納する。

#### 【0058】

メモリ部1107に格納された統合リボケーションリストを図14に示す。これにより、すべてのSTBで統合リボケーションリストを共有することが可能になる。

#### 【0059】

そして、新たなディスプレイがSTBに接続された場合に、ディスプレイから読み出したメーカーID、機器ID、Bk s vがSTBのメモリ部に保持しているリボケーションリストに同一のものがあれば、初期認証は失敗として、以降そのディスプレイを使用できなくする。

#### 【0060】

以上のように実施の形態1によれば、STBとディスプレイの初期認証処理において失敗した場合不正機器とし、その機器のメーカーIDと機器IDとKSVをSTBのメモリ部に格納してリボケーションリストを作成し、各STBからネットワークを通じてリボケーションリストをリボケーションリスト統合部にアップロードし、リボケーションリスト統合部で、各STBよりアップロードされたりボケーションリストを統合した後、セクションにパケット化し、それをTSに多重化し、多重されたTSを送信部から送出し、送信部から送出されたTSをSTBで受信し、統合リボケーションリストを取得することで、もともと各STBで個別に所有するリボケーションリストを、全てのSTBで共有することが可能となり、これにより著作権保護上、不正なディスプレイを排除し、セキュリティを

向上させることが可能となる。

#### 【0061】

##### (実施の形態2)

次に本発明のリボケーション情報の送信方法、受信方法の実施の形態2について説明する。実施の形態1と異なるのは統合リボケーションリストのパケット化の方法である。図15に実施の形態2での統合リボケーションリストを含むパケットのデータ構造を示す。実施の形態2では、図14に示すように、MPEGシステム規格のPESパケットに統合リボケーションリストを格納する。

#### 【0062】

図16に実施の形態2における統合リボケーションリストの受信フローを示す。

#### 【0063】

ステップ301において、

STBが統合リボケーションリストの格納されたPESパケットを含むTSを受信する。

#### 【0064】

ステップ302において、

STBのTSデコーダ部1104でTSから統合リボケーションリストを含むパケットを抽出するように、コントロール部1106は、TSデコーダ部1104にのPIDフィルタにRevocation\_pidを設定する。

#### 【0065】

ステップ303において、

TSデコーダ部1104で統合リボケーションリストを含むパケットを抽出し、コントロール部1106が統合リボケーションリストを取得する。

#### 【0066】

ステップ304において、

コントロール部1106は取得した統合リボケーションリストを、メモリ部107に格納する。

#### 【0067】

これにより、すべてのSTBで統合リボケーションリストを共有することが可能になる。

#### 【0068】

以上のように実施の形態2によれば、STBとディスプレイの初期認証処理において失敗した場合不正機器とし、その機器のメーカーID、機器ID、KSVをSTBのメモリ部に格納してリボケーションリストを作成し、各STBからネットワークを通じてリボケーションリストをリボケーションリスト統合部にアップロードし、リボケーションリスト統合部で各STBよりアップロードされたりボケーションリストを統合した後、PESパケットにパケット化し、それをTSに多重化し、多重化されたTSを送信部から送出し、送信部から送出されたTSをSTBで受信し、統合リボケーションリストを取得することで、もともと各STBで個別に所有するリボケーションリストを、全てのSTBで共有することが可能となり、これにより著作権保護上、不正なディスプレイを排除し、セキュリティを向上させることが可能となる。

#### 【0069】

(実施の形態3)

次に本発明のリボケーション情報の送信方法、受信方法の実施の形態3について説明する。実施の形態1と異なるのは統合リボケーションリストのパケット化の方法である。図17に実施の形態3での統合リボケーションリストを含むパケットのデータ構造を示す。実施の形態3では、図17に示すように、MPEGシステム規格のTSパケットのペイロードにPESパケットやセクション等のデータ構造をとらずにそのまま統合リボケーションリストを格納する。

#### 【0070】

図18に実施の形態3における統合リボケーションリストの受信フローを示す。

#### 【0071】

ステップ401において、

STBが統合リボケーションリストの格納されたパケットを含むTSを受信する。

**【0072】**

ステップ402において、

STBのTSデコーダ部1104でTSから統合リボケーションを含むパケットを抽出するように、コントロール部1106は、TSデコーダ部1104にのPIDフィルタにRevocation\_pidを設定する。

**【0073】**

ステップ403において、

TSデコーダ部1104で統合リボケーションリストを含むパケットを抽出し、コントロール部1106が統合リボケーションリストを取得する。

**【0074】**

ステップ404において、

コントロール部1106は取得した統合リボケーションリストを、メモリ部1107に格納する。

**【0075】**

これにより、すべてのSTBで統合リボケーションリストを共有することが可能になる。

**【0076】**

以上のように実施の形態3によれば、STBとディスプレイの初期認証処理において失敗した場合不正機器とし、その機器のメーカーID、機器ID、KSVをSTBのメモリ部に格納してリボケーションリストを作成し、各STBからネットワークを通じてリボケーションリストをリボケーションリスト統合部にアップロードし、リボケーションリスト統合部で各STBよりアップロードされたりリボケーションリストを統合した後、TSパケットのペイロードに格納することでパケット化し、それをTSに多重化し、多重化されたTSを送信部から送出し、送信部から送出されたTSをSTBで受信し、統合リボケーションリストを取得することで、もともと各STBで個別に所有するリボケーションリストを、全てのSTBで共有することが可能となり、これにより著作権保護上、不正なディスプレイを排除し、セキュリティを向上させることが可能となる。

**【0077】**

#### (実施の形態 4)

次に本発明のリボケーション情報の送信方法、受信方法の実施の形態 4 について説明する。実施の形態 1 と異なるのは、デジタル放送ではなくインターネット経由で統合リボケーションリストを各 STB に伝送することである。図 19 に実施の形態 4 におけるリボケーション情報の送信方法、受信方法を実現するシステムの構成を示す。実施の形態 1 と異なる部分についてのみ説明する。

#### 【0078】

201～203 はインターネットへのインタフェースを有する STB である。STB 201～203 の内部構成を図 20 す。図 3 に示す実施の形態 1 の STB と異なる部分についてのみ説明する。2001 は LAN I/F で後述するネットワークに接続され、IP パケットをやり取りするインタフェースである。

#### 【0079】

204～207 はインターネットによるネットワークである。208 は送出センターで、IP パケットに統合リボケーションリストするものである。209 は送信部で統合リボケーション情報が格納された IP パケットを送出するものである。

#### 【0080】

以上のように構成された実施の形態 4 についてその動作を説明する。実施の形態 1 と異なるものについて説明する。

#### 【0081】

実施の形態 4 では、STB 201～203 がリボケーションリストを作成するまでは実施の形態 1 と同一である。図 21 ボケーションリストのアップロード～送出までのフローを示す。

#### 【0082】

ステップ 501 において、

STB のコントロール部 1106 が、メモリ部 1107 に格納されたりボケーションリストからメーカー ID、機器 ID、B k s v を読み出し、LAN I/F 2001 に転送する。

#### 【0083】

ステップ502において

STBのLAN I/F2001からネットワーク204、207経由でBksvをリボケーションリスト統合部114にアップロードする。

【0084】

ステップ503において、

リボケーションリスト統合部114において、所定期間に各STBからアップロードされたBksvの一覧を作成し、これを統合リボケーションリストとする。

【0085】

ステップ504において、

リボケーションリスト統合部114から送出センター208に統合リボケーションリストを伝送する。

【0086】

ステップ505において、

送出センター208で統合リボケーションリストをIPパケットに格納する。

【0087】

ステップ506において、

送信部209より、統合リボケーションリストが格納されたIPパケットを各STBに送信する。

【0088】

ここで、ステップ505での統合リボケーションリストのパケット化について説明する。図22にIPパケットのデータ構造の一例を模式的に示す。このパケットのデータの部分に実施の形態1と同様な統合リボケーション情報を格納する。

【0089】

次に、各STBにおける統合リボケーションリストの受信の方法について説明する。図23にSTBでの統合リボケーションリストの受信フローを示す。

【0090】

ステップ601において、

STBがLAN I/F 2001で統合リボケーションリストを含むIPパケットを受信する。

【0091】

ステップ602において、

STBのコントロール部1106がLAN I/F 2001から統合リボケーションリストを抽出し、取得する。

【0092】

ステップ603において、

コントロール部1106は、取得した統合リボケーションリストをメモリ部1107に格納する。

【0093】

これにより、すべてのSTBで統合リボケーションリストを共有することが可能になる。

【0094】

そして、新たなディスプレイがSTBに接続された場合に、ディスプレイから読み出した、メーカーID、機器ID、BksvがSTBのメモリ部に保持しているリボケーションリストに同一のものがあれば、初期認証は失敗として、以降そのディスプレイを使用できなくする。

【0095】

以上のように実施の形態4によれば、STBとディスプレイの初期認証処理において失敗した場合不正機器とし、その機器のメーカーID、機器ID、KSVをSTBのメモリ部に格納してリボケーションリストを作成し、各STBからネットワークを通じてリボケーションリストをリボケーションリスト統合部にアップロードし、リボケーションリスト統合部で各STBよりアップロードされたりボケーションリストを統合した後、IPパケットにパケット化し、送信部から送出し、送信部から送出されたIPパケットをSTBで受信し、統合リボケーションリストを取得することで、もともと各STBで個別に所有するリボケーションリストを、全てのSTBで共有することが可能となり、これにより著作権保護上、不正なディスプレイを排除し、セキュリティを向上させることが可能となる。

## 【0096】

## (実施の形態5)

次に本発明のリボケーション情報の送信方法、受信方法の実施の形態5について説明する。図24に実施の形態5におけるリボケーション情報の送信方法、受信方法を実現するシステムの構成を示す。実施の形態1と異なるのは、リボケーションリストをSTBからアップロードするのではなく、リボケーションリスト統合部301で統合リボケーションリストを発行することである。リボケーションリストは、初期認証の処理が失敗の場合、ユーザがリボケーションリストを管理している機関に連絡をして、リボケーション管理機関はリボケーションリストが格納された機器を回収して、統合リボケーションリストを作成する。統合リボケーションリストは実施の形態1～3のようにTSに多重化してもよいし、実施の形態4のようにIPパケットに格納してもよい。総合リボケーションリストを作成したあとの処理は実施の形態1～4と同一である。

## 【0097】

以上のように本実施の形態5によれば、STBからリボケーションリストをアップロードすることなく、リボケーションリスト統合部で統合リボケーションリストを作成し、統合リボケーションリストをTSやIPパケットに格納し、送信部から送出し、送信部から送出されたTSをSTBで受信し、統合リボケーションリストを取得することで、もともと各STBで個別に所有するリボケーションリストを、全てのSTBで共有することが可能となり、これにより著作権保護上、不正なディスプレイを排除し、セキュリティを向上させることが可能となる。

## 【0098】

なお、以上の実施の形態の説明ではSTBをコンテンツ送出機器として説明したが、DVDやPCなど他の機器であっても構わない。またデジタルインタフェースとして、HDMIを例にとって説明したがDVIやIEEE1394であっても構わない。また、ディスプレイはAVスイッチャーなどのリピーター機器であっても構わない。また、統合リボケーションリストはTSパケットやIPパケット以外のものに格納して伝送しても構わない。またリボケーションリストをアップロードするための手段は、電話やインターネット以外のネットワークであっ



でも構わない。

#### 【0099】

##### 【発明の効果】

以上のようにこの発明によれば、著作権保護上、不正なディスプレイのリボケーションリストをSTB等の全ての映像出力機器で共有することで、不正なディスプレイを排除することが可能となり、映像出力機器とディスプレイとを接続するデジタルインタフェースのセキュリティを向上させるという効果を有する。

##### 【図面の簡単な説明】

##### 【図1】

実施の形態1～3におけるリボケーションリストの送信方法、受信方法を実現するシステムを示す図

##### 【図2】

ディスプレイの内部構成を示す図

##### 【図3】

実施の形態1～3におけるSTBの内部構成を示す図

##### 【図4】

デバイスキーの行列を示す図

##### 【図5】

初期認証の処理を示す図

##### 【図6】

STBが持つリボケーションリストを示す図

##### 【図7】

STBが持つリボケーションリストの作成のフローを示す図

##### 【図8】

更新されたりボケーションリストを示す図

##### 【図9】

実施の形態1～3におけるリボケーションリストのアップロード～統合リボケーションリスト送出までのフローを示す図

##### 【図10】

トランスポートパケットのデータ構造を模式的に示す図

【図 1 1】

トランスポートパケットのデータ構造を示す図

【図 1 2】

統合リボケーションリストをセクション構造に格納した場合のデータ構造を示す図

【図 1 3】

実施の形態 1 の統合リボケーションリストの受信フローを示す図

【図 1 4】

各 S T B で共有される統合リボケーションリストを示す図

【図 1 5】

統合リボケーションリストを P E S パケット構造に格納した場合のデータ構造を示す図

【図 1 6】

実施の形態 2 における統合リボケーションリストの受信フローを示す図

【図 1 7】

統合リボケーションリストをトランスポートパケットのペイロードに格納した場合のデータ構造を示す図

【図 1 8】

実施の形態 3 における統合リボケーションリストの受信フローを示す図

【図 1 9】

実施の形態 4 におけるリボケーションリストの送信方法、受信方法を実現するシステム装置を示す図

【図 2 0】

実施の形態 4 における S T B の内部構成を示す図

【図 2 1】

実施の形態 4 におけるリボケーションリストのアップロード～統合リボケーションリスト送出までのフローを示す図

【図 2 2】

IPパケットのデータ構造を示す図

【図 23】

実施の形態4における統合リボケーションリストの受信フローを示す図

【図 24】

実施の形態5におけるリボケーションリストの送信方法、受信方法を実現するシステム装置を示す図

【図 25】

従来例を示す図

【符号の説明】

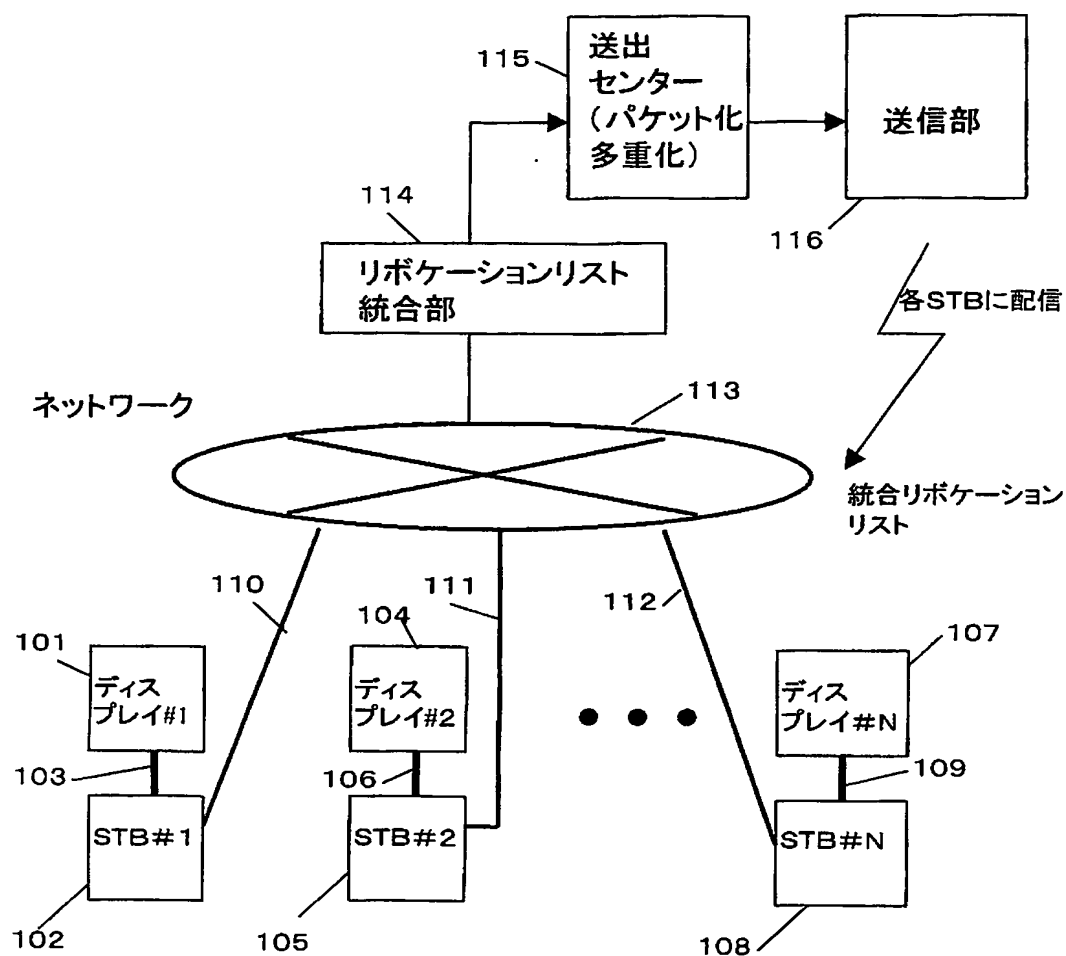
- 101 第1のディスプレイ
- 102 第1のSTB
- 103 第1のデジタルインタフェース
- 104 第2のディスプレイ
- 105 第2のSTB
- 106 第2のデジタルインタフェース
- 107 第Nのディスプレイ
- 108 第NのSTB
- 109 第Nのデジタルインタフェース
- 110 第1の上り回線
- 111 第2の上り回線
- 112 第Nの上り回線
- 113 ネットワーク
- 114 リボケーションリスト統合部
- 115 送出センター
- 116 送信部
- 1001 表示部
- 1002 機器インタフェース
- 1003 コントロール部
- 1004 メモリ部

- 1101 アンテナ
- 1102 チューナ部
- 1103 フロントエンド部
- 1104 TSデコーダ部
- 1105 AVデコーダ部
- 1106 コントロール部
- 1107 メモリ部
- 1108 ディスプレイインタフェース
- 201 第1のSTB
- 202 第2のSTB
- 203 第NのSTB
- 204～207 ネットワーク
- 208 送出センター
- 209 送信部
- 2001 LAN I/F
- 301 リボケーションリスト統合部

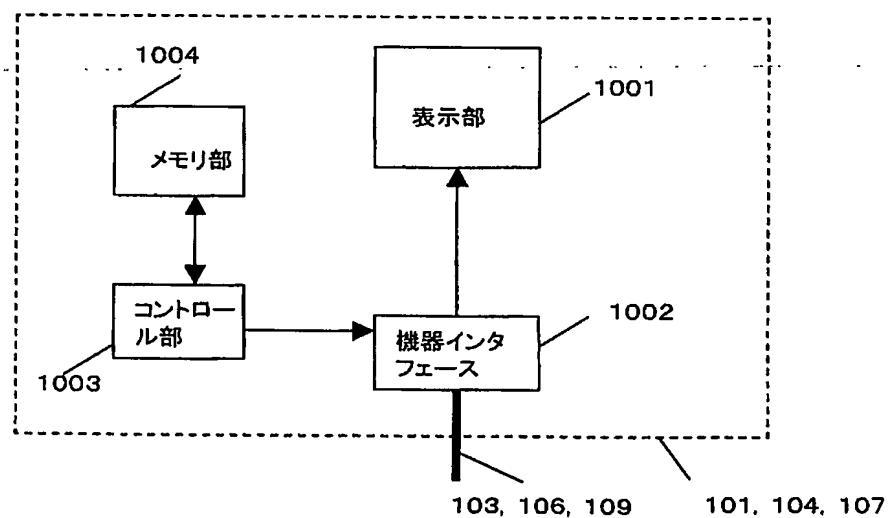
【書類名】

図面

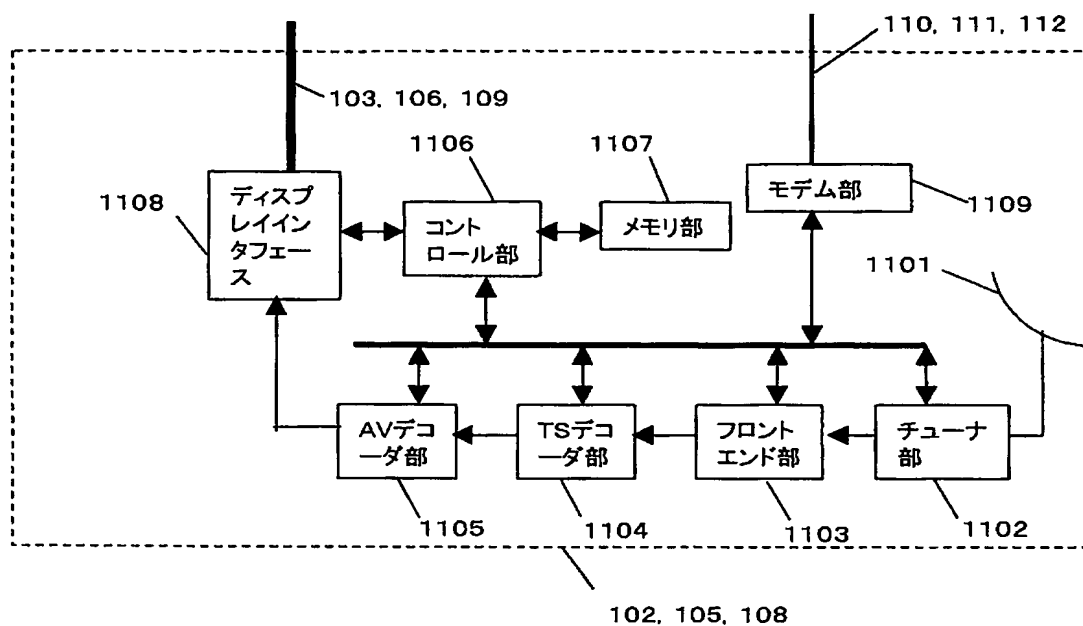
【図1】



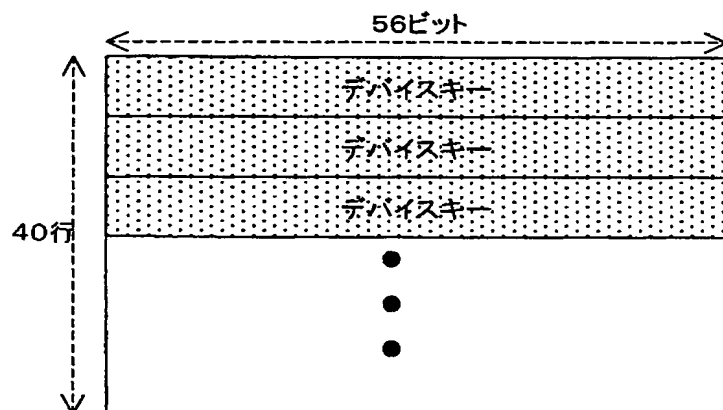
【図2】



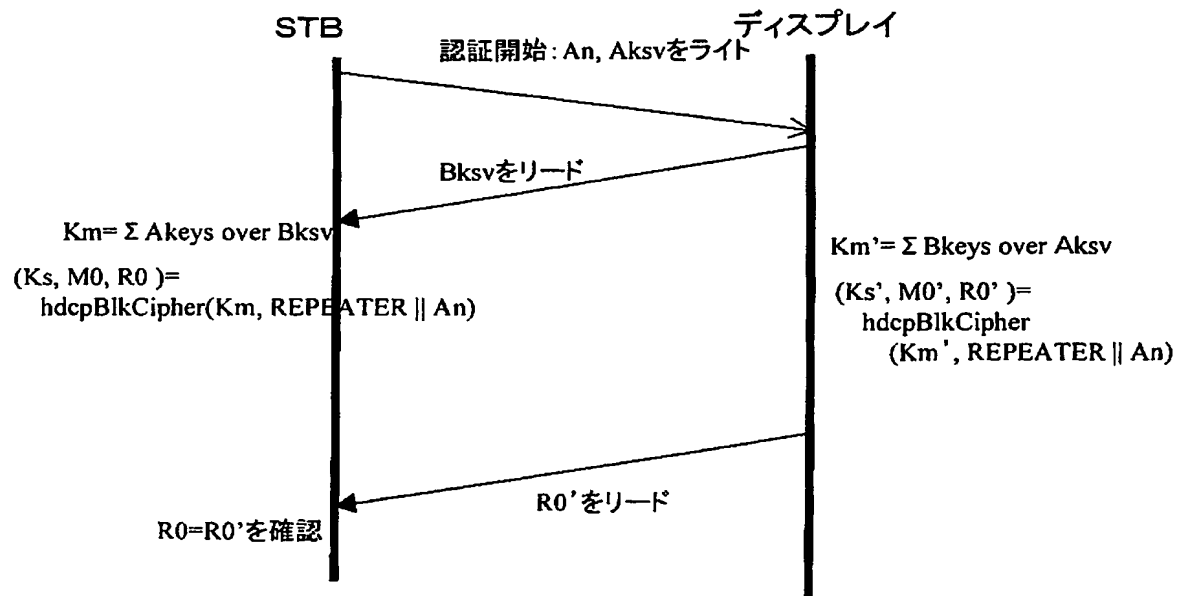
【図 3】



【図 4】



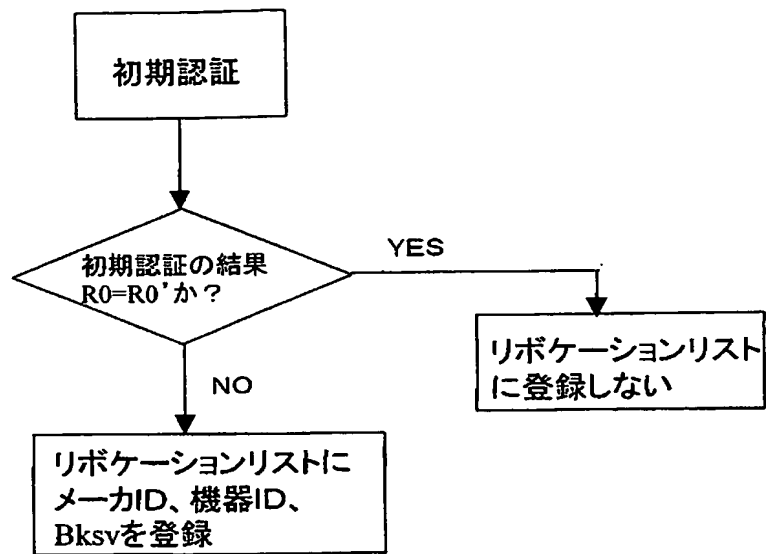
【図 5】



【図 6】

| メーカーID  | 機器ID   | Bksv   |
|---------|--------|--------|
| maker_1 | kiki_1 | Bksv_1 |
| maker_2 | kiki_2 | Bksv_2 |
| 無登録     | 無登録    | 無登録    |
| 無登録     | 無登録    | 無登録    |

【図 7】

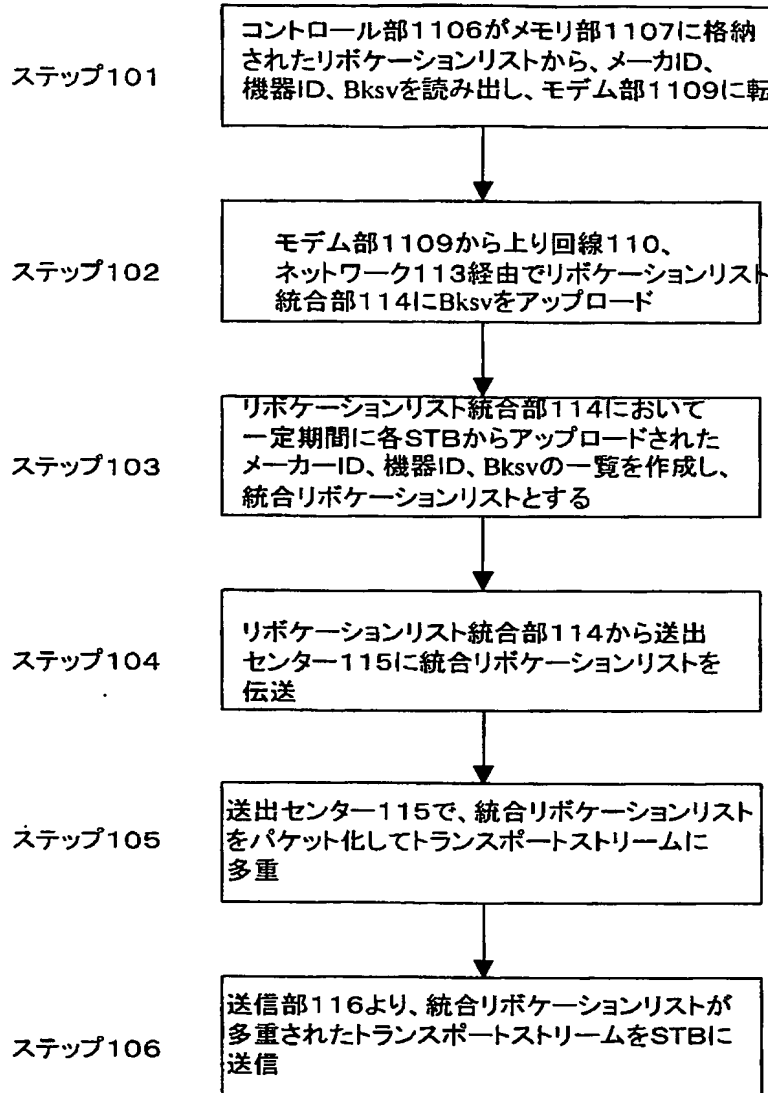


【図 8】

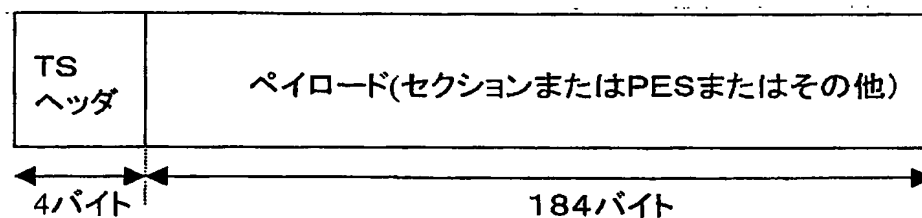
| メーカーID  | 機器ID   | Bksv   |
|---------|--------|--------|
| maker_1 | kiki_1 | Bksv_1 |
| maker_2 | kiki_2 | Bksv_2 |
| maker_3 | kiki_3 | Bksv_3 |
| 無登録     | 無登録    | 無登録    |



【図 9】



【図 10】



【図 1 1】

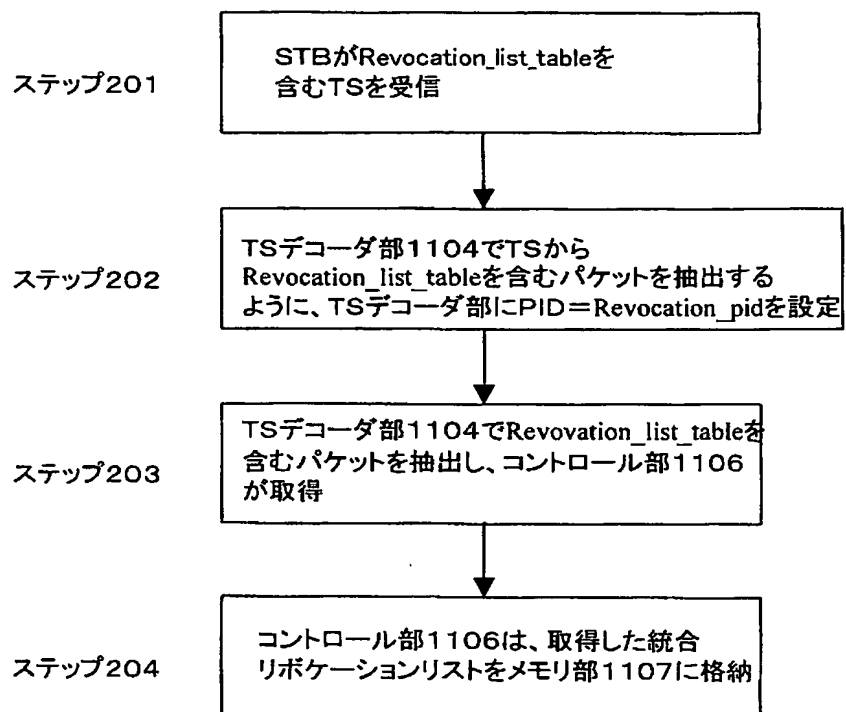
| フィールド                        | ビット数 |
|------------------------------|------|
| sync_byte                    | 8    |
| transport_stream_indicator   | 1    |
| payload_unit_start_indicator | 1    |
| transport_priority           | 1    |
| PID                          | 13   |
| transport_scrambling_control | 2    |
| adaptation_field_control     | 2    |
| continuity_counter           | 4    |
| for (i=0; i < n; i++){       |      |
| data_byte                    | 8    |
| }                            |      |

【図 1 2】

## Revocation\_List\_Table

| フィールド                    | ビット数 |
|--------------------------|------|
| table_id                 | 8    |
| section_syntax_indicator | 1    |
| reserved                 | 2    |
| section_length           | 12   |
| program_number           | 16   |
| reserved                 | 2    |
| version_number           | 5    |
| current_next_indicator   | 1    |
| section_number           | 8    |
| last_section_number      | 8    |
| for(i=0; i<n; i++){      |      |
| maker_id                 | 16   |
| kiki_id                  | 32   |
| device_KSV               | 40   |
| }                        |      |
| CRC_32                   | 32   |

【図 13】



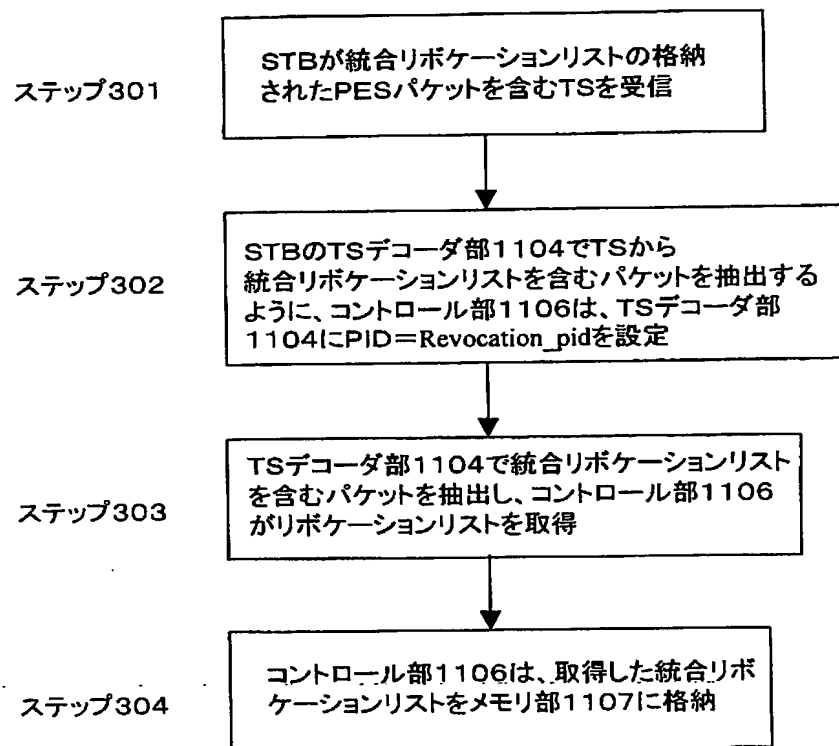
【図 14】

| メーカーID  | 機器ID   | Bksv   |
|---------|--------|--------|
| maker_1 | kiki_1 | Bksv_1 |
| maker_2 | kiki_2 | Bksv_2 |
| maker_3 | kiki_3 | Bksv_3 |
| maker_4 | kiki_4 | Bksv_4 |
| maker_5 | kiki_5 | Bksv_5 |
| 無登録     | 無登録    | 無登録    |
| 無登録     | 無登録    | 無登録    |

【図 15】

| フィールド                                  | ビット数 |
|--|------|
| packet_start_code_prefix               | 24   |
| stream_id                              | 8    |
| PES_packet_length                      | 16   |
| for (i=0; i<PES_packet_length/5; i++){ |      |
| maker_id                               | 16   |
| kiki_id                                | 32   |
| device_KSV                             | 40   |
| }                                      |      |

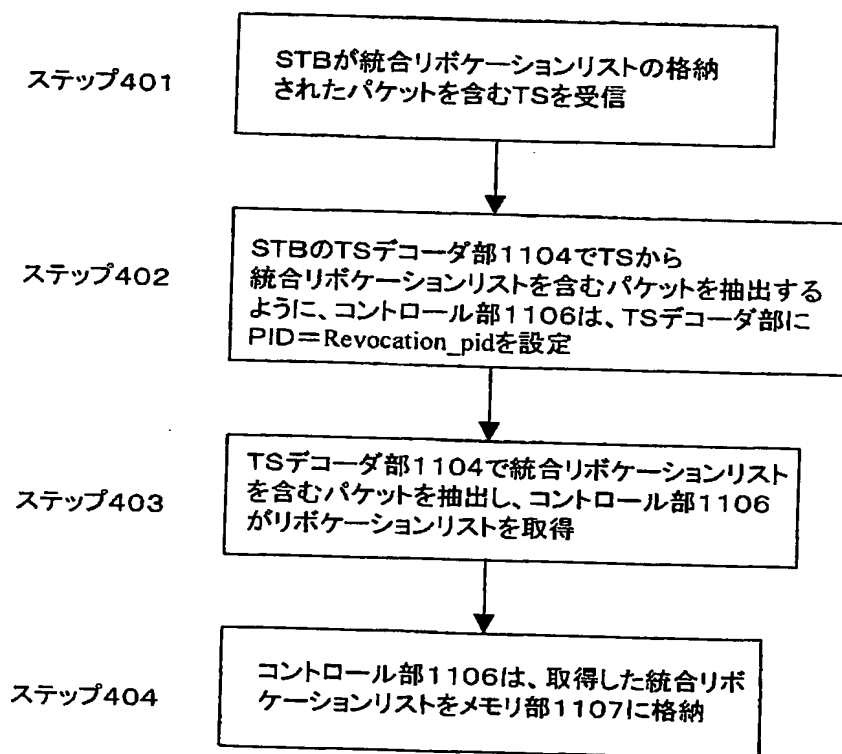
【図 16】



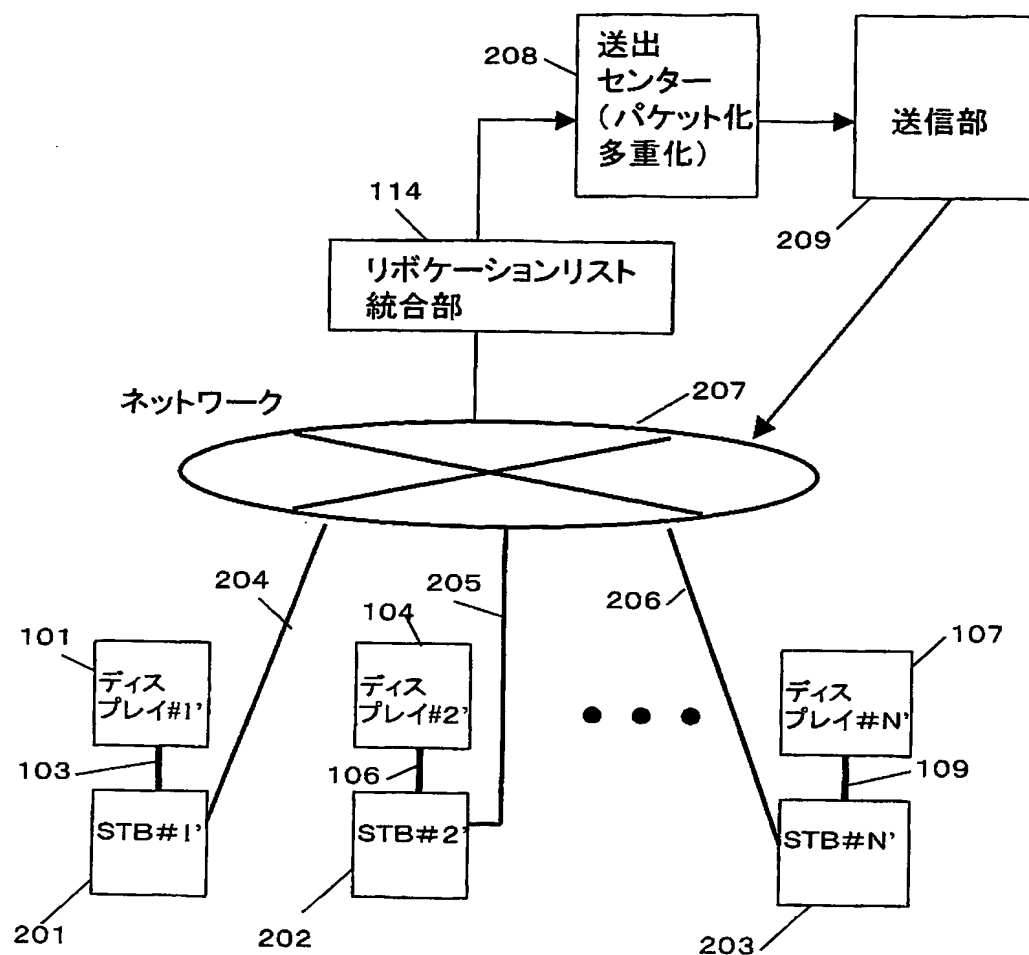
【図 17】

| フィールド                         | ビット数 |
|-------------------------------|------|
| KSV_number                    | 16   |
| For (l=0; l<KSV_number; l++){ |      |
| maker_id                      | 16   |
| kiki_id                       | 32   |
| device_KSV                    | 40   |
| }                             |      |

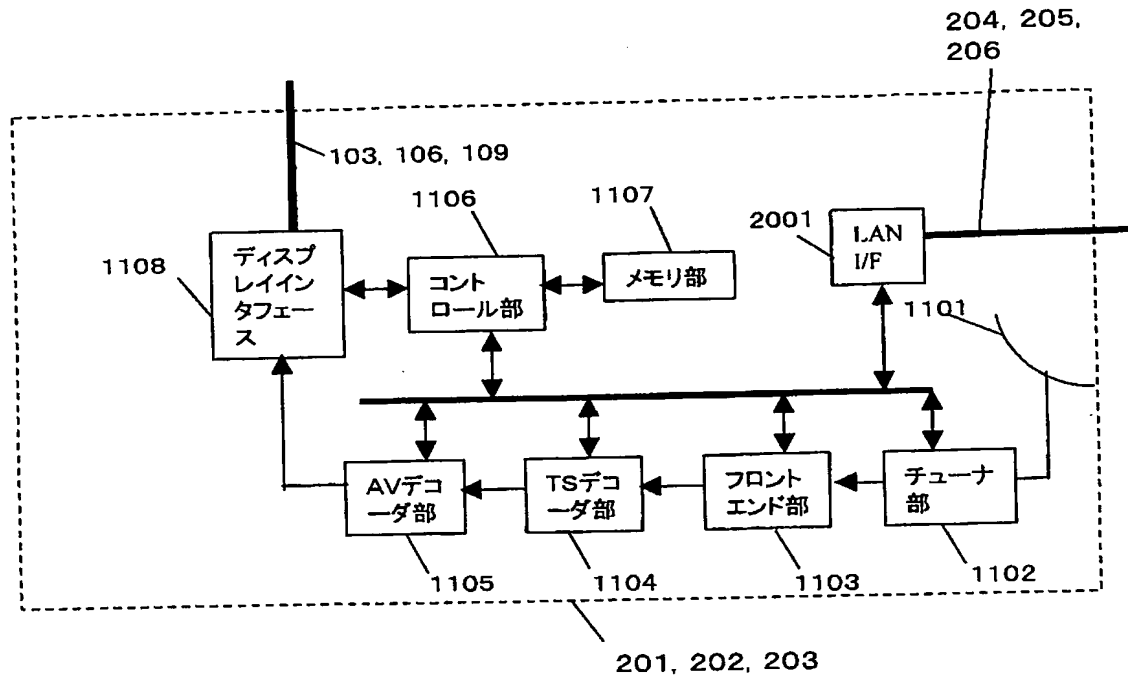
【図 18】



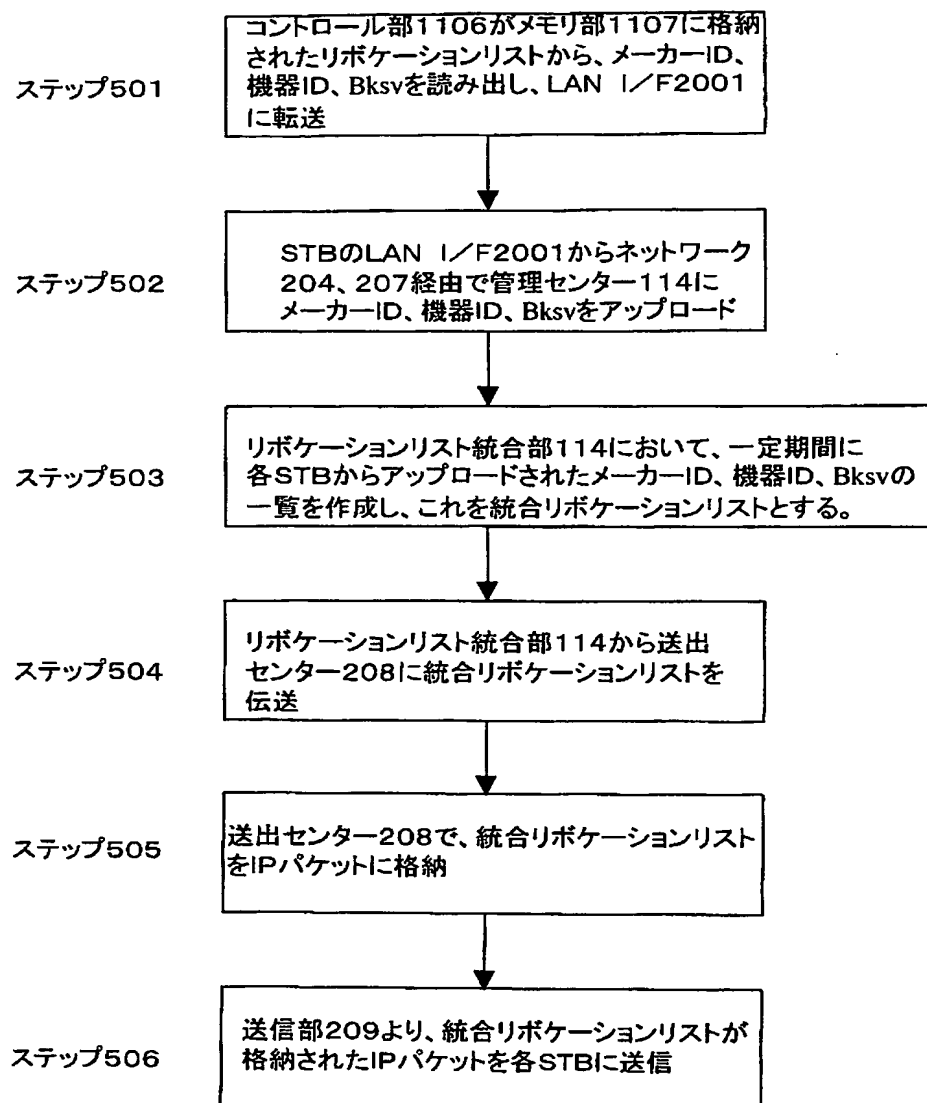
【図 19】



【図 20】



【図 21】

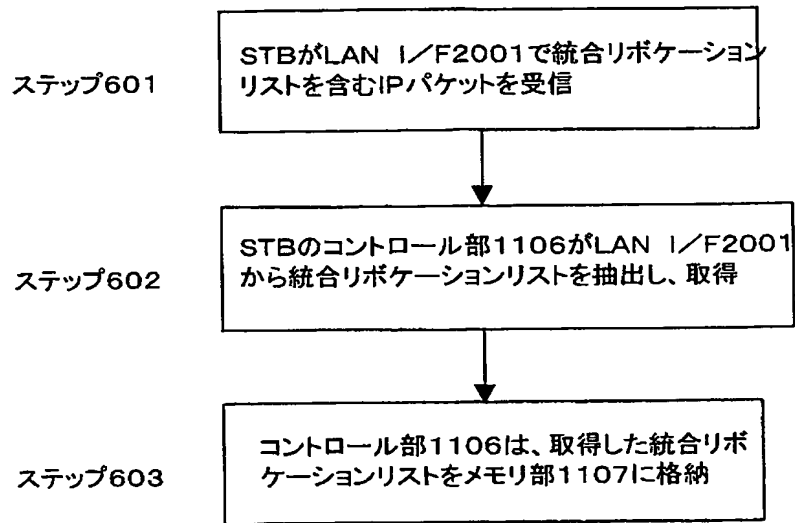


【図 22】

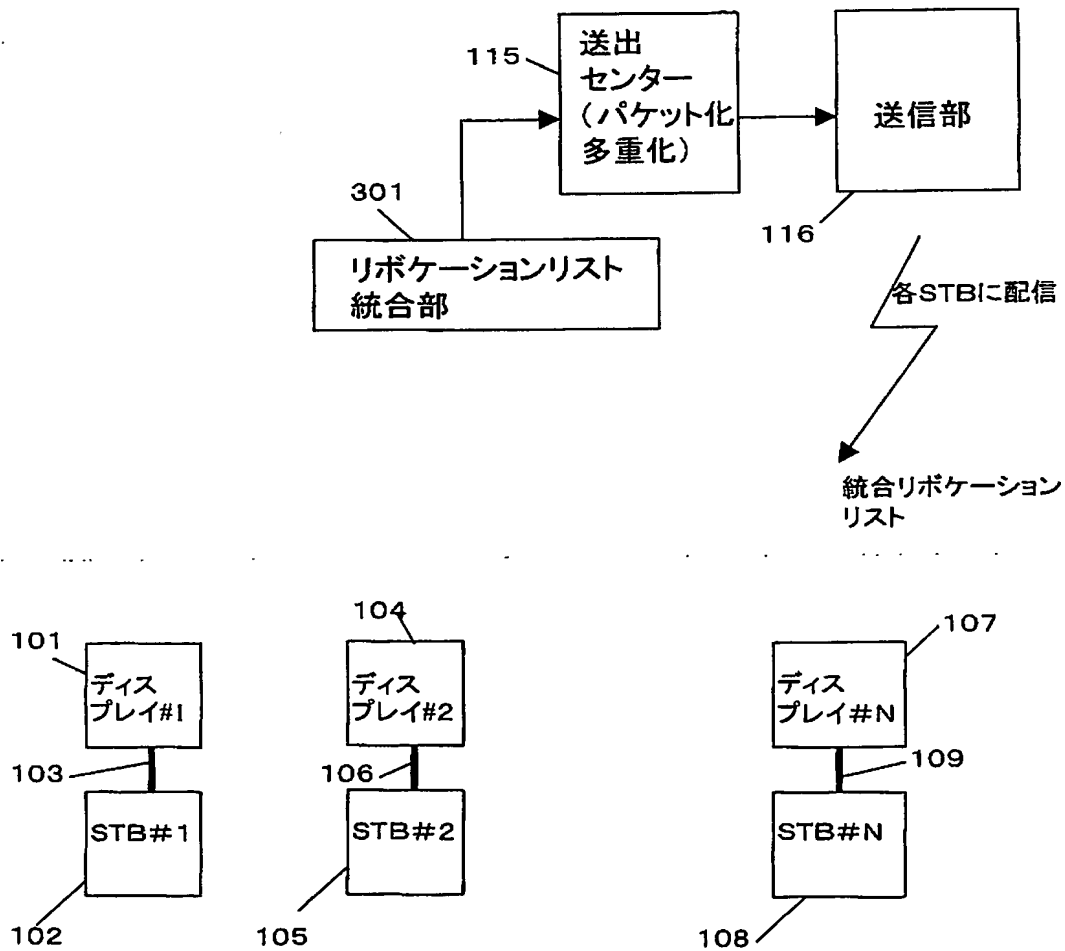
| 送信元IP<br>アドレス | 送信先IP<br>アドレス | プロトコル<br>タイプ | 送信元<br>ポート<br>番号 | 送信先<br>ポート<br>番号 | データ | FCS |
|---------------|---------------|--------------|------------------|------------------|-----|-----|
|---------------|---------------|--------------|------------------|------------------|-----|-----|



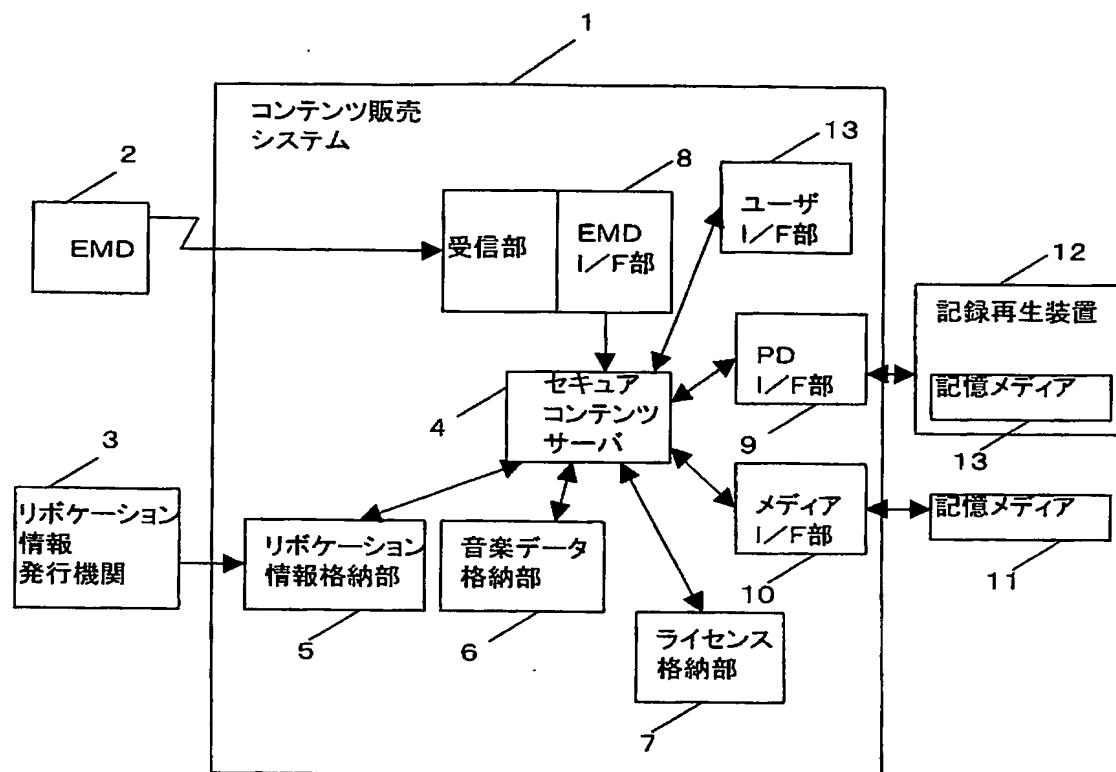
【図 2 3】



【図 2 4】



【図 25】



【書類名】 要約書

【要約】

【課題】 著作権上排除すべき不正機器のリボケーション情報はそれに接続された機器にしか記憶されない。接続されうる全ての機器に対してリボケーション情報を配布してリボケーション情報を共有して不正機器を排除する必要がある。

【解決手段】 コンテンツ送出機器／受信機器と、それらを接続する接続手段から構成されるシステムにおいて、コンテンツ送出機器とコンテンツ受信機器が相互認証を行なうステップと、相互認証が失敗の場合、失敗した鍵情報を含むリボケーション情報をネットワークにアップロードするステップと、複数のコンテンツ送出機器またはコンテンツ受信機器からアップロードされた個々のリボケーション情報を統合して統合リボケーション情報を作成するステップと、統合リボケーション情報をパケット化し、ストリームに多重するステップと、統合リボケーションが多重されたストリームを送出するステップを備えることを特徴とする。

【選択図】 図 1

特願 2 0 0 3 - 0 8 5 0 4 3

出 願 人 履 歴 情 報

識別番号

[ 0 0 0 0 0 5 8 2 1 ]

1. 変更年月日

1 9 9 0 年 8 月 2 8 日

[変更理由]

新規登録

住 所

大阪府門真市大字門真 1 0 0 6 番地

氏 名

松下電器産業株式会社